Analyst Insight

Aberdeen Group
A Harte-Hanks Company

October 2012

The Virtues of Virtual Patching

For many companies, the process of managing vulnerabilities and threats to their IT infrastructure consumes a significant portion of their limited IT resources, and keeps them painfully distracted from projects aimed at innovation and growth. The strategic deployment of selected compensating controls, such as *virtual patching*, can provide a kind of protective shield that effectively buys the organization more time to assess, plan, test and remediate vulnerabilities and threats – a potentially attractive alternative to the value-sucking activities of Patch Tuesdays, emergency patches and workarounds, endless testing, and unplanned downtime.

Business Context: Because Patching is Fast and Furious

Trying to keep up with the vulnerabilities and threats that assault enterprise IT infrastructure is a difficult but essential activity:

- **Difficult**, because dozens of critical updates and vulnerabilities are disclosed week after week, as illustrated by a typical 10-week period in the first quarter of 2012 (see Table 1)
- **Essential**, because ignoring or deferring patches or configuration changes for known vulnerabilities – in the absence of other compensating controls – is not always a responsible strategy, nor is it reasonable for most companies to disconnect their businesses from the Internet

For many companies, investments aimed at the "unrewarded" risks of vulnerabilities and threats consume a significant portion of their limited IT resources, and keeps them painfully distracted from managing the type of "rewarded" risks that really matter to management: those that try to create value for their customers and ultimately help to sustain the business.

Aberdeen's research shows that for the companies achieving best results (see the sidebar on *Determining the Best-in-Class* on page 2), the view of IT Security is *business*- and *risk-driven*, as opposed to *technology*- or *compliance-driven*. Further, once the business processes for security and compliance are accepted as tasks that must be done, the top-performing companies seek to optimize their operations for efficiency and to minimize total cost. In this way, they also help to ensure that sufficient IT resources are available to support – and ideally, to help define – management's strategic objectives for innovation and growth.

There's really no way around it: companies who want the compelling benefits of their IT computing infrastructures must also deal somehow with the corresponding vulnerabilities, threats and risks. Sources such as the National Institute of Standards and Technology (NIST) National

Analyst Insight

Aberdeen's Analyst Insights provide the analyst perspective of the research as drawn from an aggregated view of surveys, interviews, analysis and industry experience.

Definitions

Vulnerabilities are aspects of IT infrastructure that can potentially be exploited, leading to *unauthorized access*, *loss or exposure of sensitive data*, *disruption of services*, *failure to comply with regulatory requirements*, or other unwanted outcomes. Such vulnerabilities can stem from many sources, including software defects, improper configurations, and simple human error.

Aberdeen Group
A Harte-Hanks Company

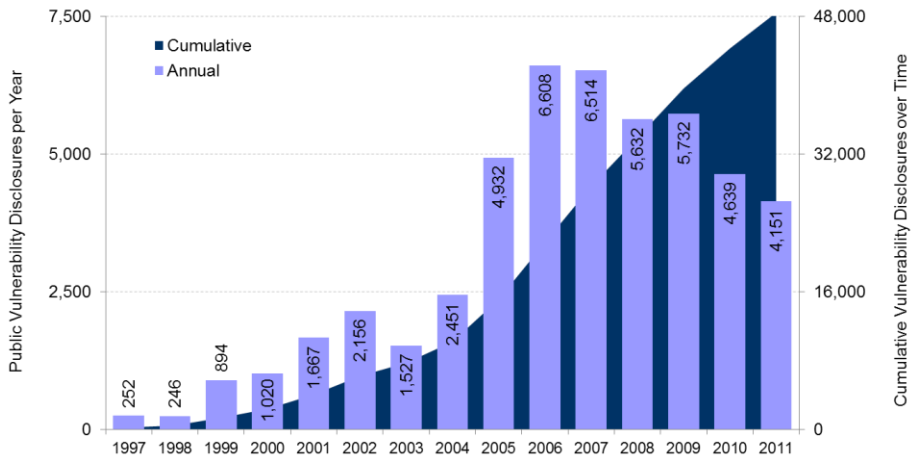
Vulnerability Database report that although the number of public vulnerability disclosures varies from year to year (see Figure 1), increasingly savvy attackers are adapting their techniques, and emerging technologies such as social, mobile and cloud are creating new avenues for attack.

Table 1: Snapshot of New Updates and Vulnerabilities in 1Q 2012

Platform		Number
Microsoft	Windows	12
	Other Microsoft Products	9
	Third Party Windows Apps	40
Mac		0
Unix	AIX	2
	BSD	1
	HP-UX	0
	Linux	12
	Novell	1
	Unix	1
Cross-Platform		74
Web Application	Web Application	46
	Web Application – Cross-Site Scripting	20
	Web Application – SQL Injection	9
Devices		17
10-Week Total		244

Data: Qualys, in cooperation with SANS, for a 10-week period in 1Q 2012
Source: Aberdeen Group, October 2012

Figure 1: Public Vulnerability Disclosures, 1997-2011



Source: NIST, *National Vulnerabilities Database* (http://nvd.nist.gov), October 2012

Determining the Best-in-Class

To distinguish Best-in-Class companies (top 20%) from Industry Average (middle 50%) and Laggard organizations (bottom 30%) in aspects of IT Security and IT GRC, Aberdeen generally uses aspects of the following:

- √ Actual security-related incidents experienced (e.g., number, year-over-year change)
- √ Audit deficiencies related to security or compliance experienced (e.g., number, year-over-year change)
- √ Annual costs related to the initiative under study

Companies with top performance based on the selected criteria earn "Best-in-Class" status.

Full details of the criteria used are provided in each respective benchmark study.

Evolving Strategies

One growing problem is that the traditional, *signature-based* approach to protecting against the vulnerabilities shown in Figure 1 is under significant stress. Most new malware represents slight variations of previously identified malware, a malevolent engineering process which is repeated continuously by attackers. The traditional approach of determining what is "good" by detecting and subtracting what is known to be "bad" is not being discarded, but increasingly it must be augmented by complementary security technologies and a *defense-in-depth* approach.

Perhaps the most disturbing insight is that the industry in general is consistently unable to keep pace with the number of vulnerabilities and threats: industry sources report that just 58% of the vulnerabilities disclosed in 2011 had vendor patches available on the same day, and **36% still had no patch available** three months into 2012. The fact that this is a slight improvement (over the past 5 years, 44% or higher of publicly disclosed vulnerabilities have had no patch available) does not change the perception that enterprises are running faster but falling further behind.

Aberdeen Research: Remediation Strategies Include Starting Sooner, Finishing Faster, Buying More Time

How can companies reduce the total economic impact of managing the threats and vulnerabilities affecting their endpoints, networks, servers and applications? Inspection of the chart in Figure 2 identifies three fundamental approaches:

1. **Start sooner** – i.e., reduce the time between the initial disclosure of threats and vulnerabilities and the initiation of remediation
2. **Finish faster** – i.e., increase the speed at which affected systems are remediated, through increased automation
3. **Buy more time** – i.e., implement additional protections (compensating controls) to allow additional time for assessing, prioritizing, and deploying patches and configuration changes for affected systems at the time most convenient for the company

Start Sooner, Finish Faster – Increasing Efficiency and Effectiveness through Automation

The financial benefits of faster time to initiation and faster time to completion for managing threats and vulnerabilities include:

- **Efficiency** – reduce the actual operational cost of vulnerability management, by leveraging automated solutions such as patch management, configuration and change management, and tools for secure software development and testing
- **Effectiveness** – move more of the costs associated with threats and vulnerabilities from the "not avoided" category to the "avoided" category, by reducing the window of vulnerability for all affected systems

Graphically, these approaches are represented in Figure 2 by the arrows labeled "*1) Start Sooner*" and "*2) Finish Faster*."

Aberdeen's research and analysis in vulnerability management – see the table of *Related Research* at the end of this report – has shown that:

- On average, about three-fourths (75%) of all companies have current deployments of *patch management*, a percentage that shows very little variation over seven studies over the last four years

- The leading performers in any given study are consistently more likely than the lagging performers to have current deployments of patch management solutions
- Current use of patch management is strongly correlated with company size – i.e., nearly all Large enterprises have deployed it, in comparison to just 3 out of 5 Small businesses

The general correlation is clear: higher adoption of patch management corresponds to a lower percentage of accepted risks. This is common sense: if you don't patch at all, you effectively accept all the risk. But even if your patching is 100%, some significant residual risks will remain. Aberdeen's analysis also shows that while current use of patch management is foundational for success, taken by itself it does not differentiate top performance – in other words, success is not only a function of *if* a company patches, but also a function of *how*.

Sector Definitions / Fast Facts

The following terms are defined by an organization's revenue in the most recent 12-month reporting period:

√ **Large:** $1B or higher

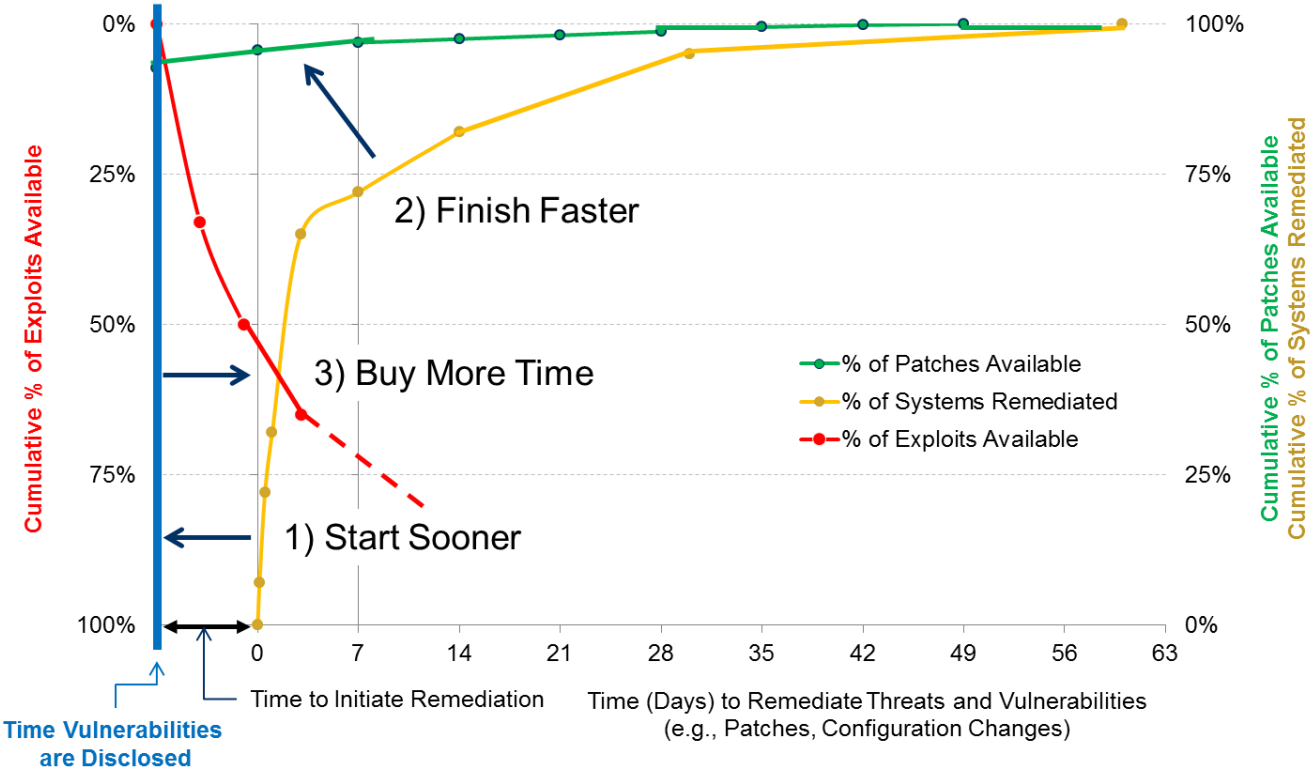
√ **Mid-Size:** less than $1B and more than $50M

√ **Small:** $50M or lower

Current deployments of *patch management*, by company size:

√ Large 96%; Mid-Size 77%; Small 64%

Figure 2: Three Approaches to Improve the Economies of Managing Threats and Vulnerabilities



Patch availability data: *2011 Trend and Risk Report*, March 2012
Source: Aberdeen Group, October 2012

Buy More Time – Prioritize and Allocate Resources through the Strategic Deployment of Compensating Controls

On the critical question of how to patch, which is the better strategy: to *start sooner* (i.e., reduce the time between the initial disclosure of

vulnerabilities and the initiation of remediation), to *finish faster* (i.e., to increase the speed at which affected systems are remediated, through increased automation) … or to *buy more time* (i.e., to implement compensating controls to allow additional time for assessing, prioritizing, and deploying patches or configuration changes for affected systems)?

The strategic deployment of selected compensating controls, such as *virtual patching*, can provide a protective shield that effectively buys the organization more time to assess, plan, test and remediate threats and vulnerabilities, as an alternative to racing to address every vulnerability on every affected endpoint, network, database, or application as quickly as possible. Graphically, this approach is represented in Figure 2 by the dashed line labeled "*3) Buy More Time*."

The Virtues of Virtual Patching

Virtual patching (sometimes referred to as *external patching*, or *vulnerability shielding*) refers to establishing a policy enforcement point that is external to the resource being protected, to identify and intercept exploits of known vulnerabilities before they reach their target. In this way, direct modifications to the resource being protected are not required.

Table 2: Scenarios When Virtual Patching Makes Sense

Scenario	Examples
Patches may not be available	▪ 36% of the vulnerabilities and threats publicly disclosed in calendar year 2011 still had no patch available at year-end
Patching may not be possible or practical	▪ Older, out of support systems ▪ Outsourced code ▪ OEM systems, e.g., where license agreements may prohibit modifications to the underlying platform
Patching takes time – and time is money	▪ The patching process itself – i.e., assessing, prioritizing, testing, remediating – is costly, especially for emergency patches or workarounds ▪ The opportunity cost of unplanned downtime, e.g., lost productivity, lost or deferred revenue, and in some cases lost customers, is prohibitive

Source: Aberdeen Group, October 2012

Table 2 provides a high-level summary of scenarios where the strategy of virtual patching makes operational and financial sense for the business:

- It buys additional time until patches are available
- It provides a compensating control when patching is not possible or practical

Fast Facts

Aberdeen's research shows that the leading performers ("Best-in-Class") are 2-times more likely than lagging performers ("Laggards") to use **virtual patching**:

√ Best-in-Class (57%)

√ Industry Average (31%)

√ Laggards (26%)

- It reduces the need for "emergency" patches or workarounds
- It requires fewer policy enforcement points (i.e., at selected points in the network, as opposed to applying a patch on every system)
- It gives enterprises the flexibility to patch on a planned schedule
- It helps to mitigate the high opportunity cost of unplanned downtime

Virtual patching can protect critical enterprise systems against vulnerabilities and zero-day attacks *temporarily*, until a patch is available and deployed – and in some cases more *permanently*, for systems that are still in service but for some reason not patchable. Virtual patching also gives the enterprise more control – the enterprise can patch on its own schedule, and avoid the value-sucking activities of Patch Tuesdays, emergency patches and workarounds, endless testing, and unplanned downtime.

To lay a simple foundation for appreciating the cost of downtime, consider just the following three broad categories: *lost revenue*, *lost productivity*, and *impact of security incidents*.

Lost Revenue

Table 3 shows the hourly impact of downtime for every $10M of annual revenue generated by a specific application or system. It also allows you to adjust for the percentage of revenue that you estimate is actually lost from an hour of downtime – e.g., for some applications, if the capacity to produce or sell is lost it can never be recovered; for others, some portion of the revenue may be lost but the rest is merely deferred.

Note that in some cases, downtime may lead to lost customers – in which case the impact is actually higher than the value of any lost transactions; the impact is the net present value of the lifetime revenue from that customer. For simplicity, this calculation has not been included in this basic analysis.

Table 3: Hourly Impact of Downtime per $10M Revenue

	Hourly Impact of Downtime per $10M Revenue									
	$114	$228	$342	$457	$571	$685	$799	$913	$1,027	$1,142
% of Revenue Lost	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%

Source: Aberdeen Group, October 2012

For example, if your website generates $20M per year in revenue, and you estimate that 80% of the revenue is truly lost, then the impact of downtime is ($20M/$10M) x $913 = $1,826 per hour. If your manufacturing system produces $100M per year, and unplanned downtime means a 100% loss of capacity, then the impact of downtime is ($100M/$10M) x $1,142 = $11,420 per hour.

Given that 1 hour of downtime per year translates roughly to 99.99% uptime, it's easy to see how these numbers can quickly grab a business leader's attention.

Lost Productivity

Table 4 shows the hourly impact of downtime for every 1,000 employees, at a fully-loaded annual cost of $100,000 per employee. As in the previous example, it allows you to adjust for the percentage of productivity that you estimate is actually lost – e.g., if the phones or email system or internet access goes down, employees may still be able to do productive work even after they break for that extra cup of coffee.

Table 4: Hourly Impact of Downtime per 1K Employees, at $100K per Employee

	Hourly Impact of Downtime per 1K Employees at $100K per Employee									
	$5,480	$10,960	$16,450	$21,930	$27,410	$32,890	$38,380	$43,860	$49,340	$54,820
% of Productivity Lost	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%

Source: Aberdeen Group, October 2012

For example, if you have 2,500 employees, an average fully-loaded cost per employee of $130K, and you estimate that 40% of their productivity is truly lost, then the impact of downtime is (2,500/1,000) x ($130K/$100K) x $21,930 = $71,273 per hour.

Given these figures as well as our own visceral experiences, it makes sense how everyone squeals when email, phone or network access goes down – but it can be confusing at how little regard is often given for the amount of productivity wasted on unnecessary meetings.

Impact of Security Incidents

In Aberdeen's research, the average total cost of a security incident – i.e., a blend of all incident types – was $130K. For application security incidents, the average total cost per incident was $300K. For incidents involving the loss or exposure of sensitive data, the average total cost per incident was as much as $640K. These cost-per-incident figures are extremely conservative in comparison to many other widely published figures, which range as high as $7M and above. Readers are encouraged to use their own estimates to personalize this simple analysis for their own business context.

Keep in mind that if your system or application is down as a direct result of a security incident, the lost revenue or lost productivity figures discussed above are merely the minimum – above and beyond that, there are still the costs of responding, remediating, communicating, making amends, and so on. Our challenge, of course, is that security-related incidents are not always as easily detected as downtime, and their financial impact is not always so easily translated into an hourly figure.

Summary and Recommendations

- Managing vulnerabilities and threats to enterprise IT infrastructure is difficult, with ongoing changes to the infrastructure itself multiplied by dozens of vulnerabilities and critical updates publicly disclosed week after week
- Ignoring or deferring patches or configuration changes for known vulnerabilities – in the absence of other compensating controls – is generally not a responsible strategy, nor is it reasonable for most companies to disconnect their businesses from the Internet
- Not patching at all means that you effectively accept all the risk, but even if your patching is 100% some significant residual risks will remain
- Patch management strategies include reducing the time between the initial disclosure of vulnerabilities and the initiation of remediation (*starting sooner*) and increasing the speed at which affected systems are remediated (*finishing faster*)
- Another important patch management strategy is to *buy more time*; *virtual patching* refers to the strategic deployment of selected compensating controls to provide a kind of protective shield that effectively buys the organization more time to assess, plan, test, and remediate threats and vulnerabilities on a schedule of their own choosing
- Virtual patching can make a strong operational and financial case for the business:
    - It buys additional time until patches are available
    - It provides a compensating control when patching is not possible or practical
    - It reduces the need for "emergency" patches or workarounds
    - It requires fewer policy enforcement points (i.e., at selected points in the network, as opposed to applying a patch on every system)
    - It gives enterprises the flexibility to patch on its own schedule
    - It helps to mitigate the high opportunity cost of unplanned downtime, which can easily range to tens of thousands of dollars per hour
- Companies should give strong consideration to virtual patching as a strategy to augment their traditional patch management processes, and to improve the overall efficiency and effectiveness of managing the vulnerabilities and threats to their IT infrastructure

Telephone: 617 854 5200
Fax: 617 723 7897

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research	
Endpoint Security: Anti-Virus Alone is Not Enough; April 2012	*Managing Vulnerabilities and Threats: No, Anti-Virus is Not Enough*; December 2010
Network Security: Firewalls Alone are Not Enough; April 2012	*Web Application Firewalls: Defend and Defer*; October 2010
To Patch, or Not to Patch? (Not If, But How); October 2011	*Making Time for Better IT Security: Sooner, Faster, Later*; August 2008
Is Your Vulnerability Management Program Leaving You at Risk? Most Likely, Yes; June 2011	*Vulnerability Management: Assess, Prioritize, Remediate, Repeat*; July 2008

Author: Derek E. Brink, Vice President and Research Fellow, IT Security and IT-GRC (Derek.Brink@aberdeen.com)